



PCT/FR 2005/050101

21 FEV. 2005

REC 15 APR 2005

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION**COPIE OFFICIELLE**

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 04 FEV. 2005

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Martine PLANCHE

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr





BREVET D'INVENTION CERTIFICAT D'UTILITE

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livre VI

REQUÊTE EN DÉLIVRANCE

DATE DE REMISE DES PIÈCES: N° D'ENREGISTREMENT NATIONAL: DÉPARTEMENT DE DÉPÔT: DATE DE DÉPÔT:	Gérard POULIN BREVALEX 3 rue du Docteur Lancereaux 75008 PARIS France
Vos références pour ce dossier: SP 24282 HM 03-021	

1 NATURE DE LA DEMANDE			
Demande de brevet			
2 TITRE DE L'INVENTION			
		PROCÉDE D'APPARIEMENT D'UN TERMINAL RECEPTEUR AVEC UNE PLURALITE DE CARTES DE CONTROLE D'ACCES	
3 DECLARATION DE PRIORITE OU REQUETE DU BENEFICE DE LA DATE DE DEPOT D'UNE DEMANDE ANTERIEURE FRANCAISE		Pays ou organisation	Date N°
4-1 DEMANDEUR			
Nom	VIACCESS		
Rue	Les Collines de l'Arche Tour Opéra C		
Code postal et ville	92057 PARIS LA DEFENSE CEDEX		
Pays	France		
Nationalité	France		
Forme juridique	Société anonyme		
5A MANDATAIRE			
Nom	POULIN		
Prénom	Gérard		
Qualité	CPI: 99 0200, Pas de pouvoir		
Cabinet ou Société	BREVALEX		
Rue	3 rue du Docteur Lancereaux		
Code postal et ville	75008 PARIS		
N° de téléphone	0153 83 94 00		
N° de télécopie	01 45 63 83 33		
Courrier électronique	brevets.patents@brevaalex.com		
6 DOCUMENTS ET FICHIERS JOINTS		Fichier électronique	Pages
Texte du brevet		textebrevet.pdf	38
Dessins		dessins.pdf	3
Désignation d'inventeurs		Détails	
		D 26, R 11, AB 1	
		page 3, figures 6, Abrégé:	
		page 3, Fig.6	

7 MODE DE PAIEMENT				
Mode de paiement		Prélèvement du compte courant		
Numéro du compte client		714		
8 RAPPORT DE RECHERCHE				
Etablissement immédiat				
9 REDEVANCES JOINTES				
	Devise	Taux	Quantité	Montant à payer
062 Dépôt	EURO	0.00	1.00	0.00
063 Rapport de recherche (R.R.)	EURO	320.00	1.00	320.00
068 Revendication à partir de la 11ème	EURO	15.00	32.00	480.00
Total à acquitter	EURO			800.00

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Signé par

Signataire: FR, Brevallex, G. Poulin

Emetteur du certificat: DE, D-Trust GmbH, D-Trust for EPO 2.0

Fonction

Mandataire agréé (Mandataire 1)



BREVET D'INVENTION

CERTIFICAT D'UTILITE

Réception électronique d'une soumission

Il est certifié par la présente qu'une demande de brevet (ou de certificat d'utilité) a été reçue par le biais du dépôt électronique sécurisé de l'INPI. Après réception, un numéro d'enregistrement et une date de réception ont été attribués automatiquement.

Demande de brevet : X

Demande de CU :

DATE DE RECEPTION	20 février 2004	Dépôt en ligne: X Dépôt sur support CD:
TYPE DE DEPOT	INPI (PARIS) - Dépôt électronique	
N° D'ENREGISTREMENT NATIONAL ATTRIBUE PAR L'INPI	0450323	
Vos références pour ce dossier	SP 24282 HM 03-021	

DEMANDEUR

Nom ou dénomination sociale	VIACCESS
Nombre de demandeur(s)	1
Pays	FR

TITRE DE L'INVENTION

PROCEDE D'APPARIEMENT D'UN TERMINAL RECEPTEUR AVEC UNE PLURALITE DE CARTES DE CONTROLE D'ACCES

DOCUMENTS ENVOYES

package-data.xml	Requetefr.PDF	fee-sheet.xml
Design.PDF	ValidLog.PDF	textebrevet.pdf
FR-office-specific-info.xml	application-body.xml	request.xml
dessins.pdf	indication-bio-deposit.xml	

EFFECTUE PAR

Effectué par:	G. Poulin
Date et heure de réception électronique:	20 février 2004 16:08:24
Empreinte officielle du dépôt	C0:FD:77:C5:FF:DC:3F:92:CA:54:35:AB:3A:18:55:EA:DE:8A:6C:0E

/ INPI PARIS, Section Dépôt /

SIEGE SOCIAL
 INSTITUT 26 bis, rue de Saint Peterbourg
 NATIONAL DE 75800 PARIS cedex 08
 LA PROPRIETE Téléphone : 01 53 04 53 04
 INDUSTRIELLE Télécopie : 01 42 93 59 30

**PROCEDE D'APPARIEMENT D'UN TERMINAL RECEPTEUR AVEC UNE
PLURALITE DE CARTES DE CONTROLE D'ACCES**

DESCRIPTION

DOMAINE TECHNIQUE

5 L'invention se situe dans le domaine de la
sécurisation de données numériques diffusées et des
équipements récepteurs destinés à recevoir ces données
dans un réseau de distribution de données et/ou
services et se rapporte plus spécifiquement à un
10 procédé d'appariement d'un équipement récepteur de
données numériques avec une pluralité de modules
externes de sécurité ayant chacun un identifiant
unique.

ÉTAT DE LA TECHNIQUE ANTÉRIEURE

15 De plus en plus d'opérateurs offrent des
données et services en ligne accessibles au moyen de
terminaux munis de processeurs de sécurité.
Généralement, les données et services distribués sont
embrouillés à l'émission par des clés secrètes et
20 désembrouillés à la réception par les mêmes clés
secrètes préalablement mises à la disposition de
l'abonné.

 Outre les techniques classiques de contrôle
d'accès basées sur l'embrouillage à l'émission et le
25 désembrouillage à la réception des données distribuées,
les opérateurs proposent des techniques basées sur
l'appariement du terminal de réception avec un
processeur de sécurité pour éviter que les données et
services distribués ne soient accessibles à des
30 utilisateurs muni d'un terminal volé ou d'un processeur

de sécurité piraté tel que par exemple une carte à puce falsifiée.

Le document WO 99/57901 décrit un mécanisme d'appariement entre un récepteur et un module de sécurité basé, d'une part, sur le chiffrement et le déchiffrement des informations échangées entre le récepteur et le module de sécurité par une clé unique stockée dans le récepteur ou dans le module de sécurité, et d'autre part, sur la présence d'un numéro de récepteur dans le module de sécurité.

Un inconvénient de cette technique provient du fait que l'association entre un récepteur et un module de sécurité qui lui est apparié est établie a priori, et qu'elle ne permet pas à l'opérateur de gérer efficacement son parc d'équipements récepteurs afin d'empêcher le détournement de cet équipement pour des utilisations frauduleuses.

Un but du procédé d'appariement selon l'invention est de permettre à chaque opérateur de limiter les utilisations de son parc de matériel de réception en configurant et en contrôlant dynamiquement l'appariement de l'équipement récepteur et des modules externes de sécurité destinés à coopérer avec cet équipement.

EXPOSÉ DE L'INVENTION

L'invention préconise un procédé d'appariement d'un équipement récepteur de données numériques avec une pluralité de modules externes de sécurité ayant chacun un identifiant unique.

Le procédé selon l'invention comporte les étapes suivantes :

- connecter un module externe de sécurité à l'équipement récepteur,
- 5 - mémoriser à la volée dans l'équipement récepteur l'identifiant unique du module de sécurité connecté.

Ce procédé comporte une phase de contrôle consistant à vérifier, à chaque connexion ultérieure d'un module externe de sécurité à l'équipement récepteur, si l'identifiant dudit module est mémorisé dans cet équipement récepteur.

A cet effet, le procédé selon l'invention comporte en outre une étape consistant à transmettre à l'équipement récepteur une signalisation comportant au moins un message de gestion de la mémorisation de l'identifiant du module externe de sécurité et/ou un message de gestion de la phase de contrôle.

Ladite signalisation comporte au moins une des consignes suivantes :

- autoriser la mémorisation,
- interdire la mémorisation,
- effacer les identifiants déjà mémorisés dans l'équipement récepteur,
- 25 - activer ou désactiver la phase de contrôle.

Dans une première variante de mise en œuvre du procédé, la signalisation comporte le nombre maximal d'identifiants dont la mémorisation est autorisée.

30 Dans une deuxième variante de mise en œuvre du procédé, ladite signalisation comporte une consigne

de reconfiguration par laquelle on transmet à l'équipement récepteur une liste mise à jour des identifiants des modules externes de sécurité appariés avec ledit équipement récepteur.

5 Ladite liste est transmise soit directement à l'équipement récepteur, soit via un module externe de sécurité connecté audit équipement récepteur.

 Préférentiellement, ladite phase de contrôle comporte une procédure consistant à perturber
10 le traitement des données si l'identifiant du module externe de sécurité connecté n'est pas préalablement mémorisé dans l'équipement récepteur.

 Le procédé selon l'invention s'applique lorsque les données sont distribuées en clair et
15 également lorsque ces données sont distribuées sous forme embrouillée par un mot de contrôle chiffré. Dans ce dernier cas, chaque module externe de sécurité comporte des droits d'accès auxdites données et un algorithme de déchiffrement dudit mot de contrôle pour
20 désembrouiller les données.

 La signalisation de contrôle est transmise dans un message EMM (Entitlement Management Message, en anglais) spécifique à un module externe de sécurité associé à cet équipement récepteur ou dans un message
25 EMM spécifique à cet équipement récepteur, et pour un équipement récepteur donné, la liste mise à jour des identifiants des modules externes de sécurité appariés avec cet équipement récepteur est également transmise dans un message EMM spécifique à un module de sécurité
30 associé à cet équipement récepteur.

Alternativement, ladite signalisation est transmise dans un flux privé à un groupe d'équipements récepteurs, et la liste mise à jour des identifiants des modules externes est également transmise dans un flux privé à chaque équipement récepteur. Dans ce dernier cas, ledit flux privé est traité par un logiciel dédié exécutable dans chaque équipement récepteur en fonction de l'identifiant du module externe de sécurité qui lui est associé.

Dans une autre variante, la signalisation est transmise à un groupe d'équipements récepteurs dans un message EMM spécifique à un groupe de modules externes de sécurité associés auxdits équipements récepteurs ou dans un message EMM spécifique audit groupe d'équipements récepteurs, et pour un groupe d'équipements récepteurs donné, la liste mise à jour des identifiants des modules externes est transmise dans un message EMM spécifique à un groupe de modules externes de sécurité associés auxdits équipements récepteurs.

Par ailleurs, pour un groupe d'équipements récepteurs donné, la signalisation de contrôle et la liste mise à jour peuvent également être transmises à un groupe d'équipements dans un flux privé.

Dans ce cas, ledit flux privé est traité par un logiciel dédié exécutable dans chaque équipement récepteur en fonction de l'identifiant du module externe de sécurité qui lui est associé.

Lorsque la transmission de la signalisation et des listes mises à jour est effectuée par des EMM, le procédé comporte un mécanisme destiné à empêcher

l'utilisation d'un EMM transmis à un même module de sécurité dans deux équipements récepteurs distincts.

Les EMM spécifiques à un module de sécurité ou à un équipement récepteur présentent le format
5 suivant :

```

EMM-U_section() {
  table_id = 0x88                8 bits
  section_syntax_indicator = 0   1 bit
  DVB_reserved                   1 bit
10  ISO_reserved                 2 bits
  EMM-U_section_length           12 bits
  unique_adress_field            40 bits
  for (i=0; i<N; i++) {
    EMM_data_byte                8 bits
15    }
  }

```

Les EMM spécifiques à tous les modules externes de sécurité ou à tous les équipements récepteurs présentent le format suivant :

```

20  EMM-G_section() {
    table_id = 0x8A ou 0x8B      8 bits
    section_syntax_indicator = 0 1 bit
    DVB_reserved                 1 bit
    ISO_reserved                 2 bits
25  EMM-G_section_length         12 bits
    for (i=0; i<N; i++) {
      EMM_data_byte              8 bits
    }
  }

```

30 Les EMM spécifiques à un sous-groupe de modules externes de sécurité ou à un sous-groupe d'équipements récepteurs présentent le format suivant :

```

EMM-S_section() {
    table_id = 0x8E                8 bits
    section_syntax_indicator = 0   1 bit
    DVB_reserved                   1 bit
5    ISO_reserved                  2 bits
    EMM-S_section_length           12 bits
    shared_address_field           24 bits
    reserved                       6 bits
    data_format                    1 bit
10   ADF_scrambling_flag           1 bit
    for (i=0; i<N; i++) {
        EMM_data_byte              8 bits
    }
}

```

15 Selon une caractéristique supplémentaire,
les identifiants de modules de sécurité sont groupés
dans une liste chiffrée.

Le procédé peut être utilisé dans une
première architecture dans laquelle l'équipement
20 récepteur comporte un décodeur et le module de sécurité
comporte une carte de contrôle d'accès dans laquelle
sont mémorisées des informations relatives aux droits
d'accès d'un abonné à des données numériques
distribuées par un opérateur.

25 Dans cette architecture, l'appariement est
effectué entre le décodeur et la carte de contrôle
d'accès.

Le procédé peut être utilisé dans une
deuxième architecture dans laquelle l'équipement
30 récepteur comporte un décodeur et le module de sécurité
comporte une interface de sécurité amovible munie d'une
mémoire non volatile et destinée à coopérer, d'une

part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur.

5 Dans cette architecture, l'appariement est effectué entre ledit décodeur et ladite interface de sécurité amovible.

10 Le procédé peut être utilisé dans une troisième architecture dans laquelle l'équipement récepteur comporte un décodeur muni d'une interface de sécurité amovible ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel.

15 Dans cette architecture, l'appariement est réalisé entre ladite interface de sécurité amovible et lesdites cartes de contrôle d'accès.

20 Dans une application particulière du procédé selon l'invention, les données sont des programmes audiovisuels.

25 Le procédé selon l'invention est mis en œuvre dans un système comportant une pluralité d'équipements récepteurs connectés à un réseau de diffusion de données et/ou services, chaque équipement récepteur étant susceptible d'être apparié avec une pluralité de modules externes de sécurité, ce système comportant également une plateforme de gestion commerciale communiquant avec lesdits équipements récepteurs et avec lesdits modules externes de
30 sécurité. Ce système comporte en outre :

- un premier module agencé dans ladite plate-forme de gestion commerciale et destiné à générer des requêtes d'appariement,

5 - et un deuxième module agencé dans lesdits équipements récepteurs et destiné à traiter lesdites requêtes pour préparer une configuration de l'appariement et pour contrôler cet appariement.

10 L'invention concerne également un équipement récepteur susceptible d'être apparié avec une pluralité de modules externes de sécurité pour gérer l'accès à des données numériques distribuées par un opérateur.

15 Selon l'invention, cet équipement comporte des moyens pour mémoriser à la volée l'identifiant de chaque module externe de sécurité qui lui est connecté.

20 Dans un premier mode de réalisation, l'équipement récepteur comporte un décodeur et le module externe de sécurité est une carte de contrôle d'accès comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques, l'appariement étant effectué entre ledit décodeur et ladite carte.

25 Dans un deuxième mode de réalisation, l'équipement comporte un décodeur et le module externe de sécurité est une interface de sécurité amovible munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel, pour gérer l'accès auxdites données numériques, l'appariement étant effectué entre ledit
30 décodeur et ladite interface de sécurité amovible.

Dans un troisième mode de réalisation, l'équipement comporte un décodeur muni d'une interface de sécurité amovible ayant une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel et l'appariement est réalisé entre ladite interface de sécurité amovible et lesdites cartes de contrôle d'accès.

L'invention concerne également un décodeur susceptible de coopérer avec une pluralité de modules externes de sécurité pour gérer l'accès à des programmes audiovisuels distribués par un opérateur, chaque module externe de sécurité ayant un identifiant unique et comportant au moins un algorithme de traitement de données.

Le décodeur selon l'invention comporte des moyens pour mémoriser à la volée l'identifiant de chaque module externe de sécurité qui lui est connecté.

Dans un premier mode de réalisation, lesdits modules externes de sécurité sont des cartes de contrôle d'accès dans lesquelles sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur.

Dans un deuxième mode de réalisation, lesdits modules externes de sécurité sont des interfaces de sécurité amovibles comportant une mémoire non volatile et destinées à coopérer, d'une part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur.

L'invention concerne également une interface de sécurité amovible comportant une mémoire non volatile et destinée à coopérer, d'une part, avec un équipement récepteur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel, pour gérer l'accès à des données numériques distribuées par un opérateur, chaque carte ayant un identifiant unique et comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques.

L'interface selon l'invention comporte des moyens pour enregistrer à la volée l'identifiant de chaque carte de contrôle d'accès dans ladite mémoire non volatile.

Dans une première variante, cette interface est une carte PCMCIA (pour Personal Computer Memory Card International Association) comportant un logiciel de désembrouillage de données numériques.

Dans une deuxième variante, cette interface est un module logiciel qui peut être exécuté soit dans l'équipement récepteur soit dans le module externe de sécurité.

L'invention concerne en outre un programme d'ordinateur exécutable dans un équipement récepteur susceptible de coopérer avec une pluralité de modules externes de sécurité ayant chacun un identifiant unique et dans lesquels sont stockées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur.

Ce programme d'ordinateur comporte des instructions pour mémoriser à la volée l'identifiant de chaque module externe de sécurité connecté audit

équipement récepteur et des instructions destinées à générer localement des paramètres de contrôle de l'appariement de l'équipement récepteur avec un module externe de sécurité en fonction d'une signalisation transmise audit équipement récepteur par l'opérateur.

Ce Programme d'ordinateur comporte en outre des instructions destinées à vérifier, à chaque utilisation ultérieure d'un module externe de sécurité avec l'équipement récepteur, si l'identifiant dudit module externe de sécurité est mémorisé dans l'équipement récepteur.

BREVE DESCRIPTION DES DESSINS

D'autres caractéristiques et avantages de l'invention ressortiront de la description qui va suivre, prise à titre d'exemple non limitatif en référence aux figures annexées dans lesquelles :

- la figure 1 représente une première architecture pour la mise en œuvre de l'appariement selon l'invention,

- la figure 2 représente une deuxième architecture pour la mise en œuvre de l'appariement selon l'invention,

- la figure 3 représente une troisième architecture pour la mise en œuvre de l'appariement selon l'invention,

- la figure 4 représente la structure des messages EMM de configuration et d'utilisation des fonctionnalités d'appariement selon l'invention

- la figure 5 représente un diagramme d'état de la fonction d'appariement selon l'invention,

- la figure 6 représente un organigramme illustrant un mode particulier de mise en œuvre de l'appariement selon l'invention.

5 EXPOSÉ DÉTAILLÉ DE MODES DE RÉALISATION PARTICULIERS

L'invention va maintenant être décrite dans le cadre d'une application dans laquelle un opérateur diffusant des programmes audiovisuels met en œuvre le procédé selon l'invention pour limiter l'utilisation de son parc d'équipements récepteurs à ses propres abonnés.

Le procédé peut être mis en œuvre dans trois architectures distinctes illustrées respectivement par les figures 1, 2 et 3. Les éléments identiques dans ces trois architectures seront désignés par des références identiques.

La gestion de l'appariement est réalisée à partir d'une plateforme commerciale 1 contrôlée par l'opérateur et communiquant avec l'équipement récepteur installé chez l'abonné.

Dans la première architecture, illustrée par la figure 1, l'équipement récepteur comporte un décodeur 2 dans lequel est installé un logiciel de contrôle d'accès 4, et le module externe de sécurité est une carte de contrôle d'accès 6 comportant des informations relatives aux droits d'accès d'un abonné aux programmes audiovisuels diffusés. Dans ce cas, l'appariement est effectué entre le décodeur 2 et ladite carte 6.

Dans la deuxième architecture illustrée par la figure 2, l'équipement récepteur comporte un

décodeur 2, non dédié au contrôle d'accès, et le module externe de sécurité est une interface de sécurité amovible 8 munie d'une mémoire non volatile et dans laquelle est installé le logiciel de contrôle d'accès 4. Cette interface 8 coopère, d'une part, avec ledit

Dans cette architecture, l'appariement est réalisé entre ladite interface de sécurité amovible 8 et ladite carte de contrôle d'accès 6.

Dans la troisième architecture, illustrée par la figure 3, l'équipement récepteur comporte un décodeur 2 dans lequel est installé un logiciel de contrôle d'accès 4, ce décodeur 2 est connecté à une interface de sécurité amovible 8 ayant une mémoire non volatile qui coopère avec une carte 6 parmi une pluralité de cartes de contrôle d'accès conditionnel.

Dans ce cas, l'appariement est effectué entre le décodeur 2 et l'interface de sécurité amovible 8.

La configuration et l'utilisation par l'opérateur de l'appariement résulte de commandes émises par la plateforme de gestion commerciale 1.

La description qui suit concerne la mise en oeuvre de l'invention dans le cas d'appariement d'un décodeur 2 avec une carte 6. Les étapes mises en oeuvre s'appliquent aux trois architectures décrites ci-dessus.

A la sortie d'usine d'un décodeur 2, comme après un téléchargement du logiciel de contrôle d'accès

4 dans ce décodeur, tous les traitements de l'appariement sont inactifs. En particulier :

- aucun identifiant de carte n'est mémorisé dans le décodeur 2,

5 - le nombre maximal d'identifiants de cartes mémorisables n'est pas initialisé,

- la mémorisation par le décodeur 2 de l'identifiant d'une carte 6 n'est pas active,

10 - le contrôle par le décodeur 2 de l'identifiant d'une carte 6 n'est pas actif.

Lorsqu'une carte valide est insérée dans le lecteur de carte prévu à cet effet dans le décodeur 2, l'appariement entre cette carte et le décodeur 2 peut alors être configuré par une requête de l'opérateur sur la plateforme de gestion 1 qui émet vers le décodeur 2 un message de gestion EMM dédié à l'appariement. Ce message de gestion EMM est adressé directement au décodeur 2 ou indirectement via la carte 6. Ce message de gestion EMM permet de réaliser les tâches suivantes :

20 - activer dans le décodeur 2 la fonction d'appariement ; dans ce cas le décodeur 2 vérifie si l'identifiant de la carte 6 fait partie des identifiants qu'il a mémorisés. Si ce n'est pas le cas, et si le nombre maximal d'identifiants de cartes mémorisables n'est pas atteint, le décodeur mémorise l'identifiant de cette carte.,

25 - désactiver dans le décodeur la fonction d'appariement. Dans ce cas le décodeur ne contrôle pas et ne mémorise pas l'identifiant de la carte 6,

30

- effacer les identifiants de cartes déjà mémorisés dans le décodeur.

- définir le nombre maximal d'identifiants de cartes mémorisables par le décodeur.

5 En outre l'opérateur peut émettre via la plateforme 1, un message EMM contenant une liste imposée des identifiants de cartes 6 appariées à un décodeur 2. Un tel message est adressé au décodeur 2 indirectement via la carte 6.

10 ADRESSAGE DES MESSAGES EMM

 Les messages EMM permettant la configuration et l'utilisation des fonctionnalités liées à l'appariement selon le procédé de l'invention sont émis dans une voie EMM d'un multiplex numérique tel que défini par le standard MPEG2/Système et les
15 standards DVB/ETSI.

 Cette voie peut diffuser des EMM référençant une adresse de carte(s) permettant de les destiner :

20 - au décodeur dans lequel est insérée une carte particulière,

 - aux décodeurs dans lesquels sont insérées les cartes d'un groupe particulier,

25 - aux décodeurs dans lesquels sont insérées toutes les cartes.

 Ces EMM destinés aux décodeurs « via la carte » sont utilisés notamment quand les décodeurs ne disposent pas d'adresse.

30 Cette voie peut diffuser également des EMM référençant une adresse de décodeur(s) permettant de les destiner directement :

- à un décodeur particulier,
- à un groupe particulier de décodeurs,
- à tous les décodeurs ;

5 Les EMM directement destinés à tous les décodeurs sont utilisables également quand les décodeurs ne disposent pas d'adresse.

Les messages destinés à un décodeur désigné par une carte particulière ou directement à un décodeur
10 particulier sont des EMM-U présentant la structure suivante :

```

EMM-U_section() {
    table_id = 0x88                8 bits
    section_syntax_indicator = 0   1 bit
15  DVB_reserved                   1 bit
    ISO_reserved                   2 bits
    EMM-U_section_length           12 bits
    unique_adress_field            40 bits
    for (i=0; i<N; i++) {
20      EMM_data_byte              8 bits
    }
}
```

Le paramètre unique_adress_field est
25 l'adresse unique d'une carte dans un EMM-U carte ou l'adresse unique d'un décodeur dans un EMM-U décodeur

Les messages destinés à des décodeurs désignés par un groupe particulier de cartes ou directement à un groupe particulier de décodeurs sont
30 des EMM-S présentant la structure suivante :

```

    EMM-S_section() {
        table_id = 0x8E                8 bits
        section_syntax_indicator = 0   1 bit
5      DVB_reserved                    1 bit
        ISO_reserved                    2 bits
        EMM-S_section_length           12 bits
        shared_address_field           24 bits
        reserved                        6 bits
10     data_format                     1 bit
        ADF_scrambling_flag            1 bit
        for (i=0; i<N; i++) {
            EMM_data_byte               8 bits
        }
15     }

```

Le paramètre `shared_adress_field` est l'adresse du groupe de cartes dans un EMM-S carte ou l'adresse du groupe de décodeurs dans un EMM-S
 20 décodeur. Un décodeur d'un groupe ou une carte d'un groupe est concerné(e) par le message si en outre il (elle) est explicitement désigné(e) dans un champ ADF contenu dans `EMM_data_byte` et pouvant être chiffré selon l'information `ADF_scrambling_flag`.

25

Les messages destinés aux décodeurs désignés par toutes les cartes ou directement à tous les décodeurs sont des EMM-G présentant la structure suivante :

30

```

    EMM-G_section() {
        table_id = 0x8A ou 0x8B           8 bits
        section_syntax_indicator = 0      1 bit
5       DVB_reserved                      1 bit
        ISO_reserved                      2 bits
        EMM-G_section_length             12 bits
        for (i=0; i<N; i++) {
            EMM_data_byte                 8 bits
10          }
        }
    }

```

CONTENU DES MESSAGES EMM

La figure 4 illustre schématiquement le contenu des données EMM_data_byte d'un message EMM d'appariement. Ce contenu dépend de la fonction à exécuter par le décodeur 2 pour la configuration ou l'utilisation de l'appariement.

Les données EMM_data_byte incluent les paramètres fonctionnels suivants :

- ADF 20: complément d'adressage d'un décodeur dans un groupe de décodeurs ; ce paramètre est utile en cas d'adressage par groupe sinon il peut être omis ; il peut être chiffré,
- 25 - SOID 22 : identification de messages d'appariement selon l'invention, parmi d'autres types de messages,
- OPID/NID 24 : identification du parc de décodeurs et du signal de l'opérateur,
- 30 - TIME 26 : données d'horodatage de l'émission du message ; ce paramètre est utilisé pour éviter le rejeu du message par un même décodeur,

- CRYPTO 28 : identification des fonctions de protection cryptographique appliquées aux paramètres FUNCTIONS 32.

5 Les paramètres FUNCTIONS peuvent être chiffrés et protégés par une redondance cryptographique 30.

- FUNCTIONS 32 : ensemble des paramètres décrivant la configuration et l'utilisation de l'appariement.

10 Les paramètres fonctionnels ci-dessus sont organisés librement dans les données EMM_data_byte d'un message EMM. Une implémentation préférée est la combinaison de ces paramètres par structure T L V (Type Longueur Valeur).

15

TRAITEMENT DES MESSAGES EMM

Les paramètres fonctionnels ci-dessus sont destinés à être traités par le décodeur 2.

20 Quand ils sont transmis dans un EMM décodeur, ces paramètres constituent le contenu utile de l'EMM.

25 Quand ils sont transmis dans un EMM carte, ces paramètres constituent une partie, clairement identifiable par la carte, du contenu utile de l'EMM qui contient d'autres paramètres concernant la carte. Cette dernière se charge alors d'extraire les paramètres fonctionnels qui le concernent de l'EMM et de les transmettre au décodeur 2. Une réalisation préférée pour permettre ce mécanisme de tri consiste à
30 intégrer ces paramètres fonctionnels dans un paramètre d'encapsulation non traitable par la carte. Ainsi, à la

détection par la carte 6 de cette encapsulation, la carte 6 envoie au décodeur 2 une réponse de type « Paramètre Non Interprétable (PNI) » accompagnée de l'ensemble des paramètres du décodeur 2.

5 La carte 6 reçoit également un ordre daté d'inscription de données via un EMM carte, permettant, d'une part, de s'assurer que la carte 6 n'a pas déjà traité ce message dans un autre décodeur, afin d'éviter le rejeu sur un autre décodeur et, d'autre part, de
10 limiter le traitement de cet EMM par un seul décodeur. Sémantiquement ces données signifient « Déjà traité ». Une réalisation préférée de ce mécanisme d'anti-rejeu est l'inscription de ces données d'anti-rejeu dans un bloc de données FAC (Facilities Data Block en anglais)
15 de la carte.

Si suite au traitement d'un EMM_carte d'appariement la carte répond « PNI » et « Déjà Traité » le décodeur 2 ne prend pas en compte les paramètres qu'il reçoit.

20 CONFIGURATION ET UTILISATION DE L'APPARIEMENT

L'ensemble des paramètres FUNCTIONS 32 décrit la configuration et l'utilisation de l'appariement selon l'invention. Cet ensemble de paramètres est une combinaison quelconque des
25 paramètres fonctionnels suivants :

- MODE : ce paramètre active, désactive ou réinitialise la solution d'appariement. Après désactivation, le décodeur ne contrôle pas l'identifiant d'une carte insérée dans le décodeur mais
30 conserve la liste des identifiants déjà mémorisés, et après réinitialisation, le décodeur ne contrôle pas

l'identifiant d'une carte insérée et n'a plus d'identifiant de cartes mémorisé.

5 - NBCA (Nombre de cartes autorisées) : ce paramètre impose le nombre maximal d'identifiants de cartes qu'un décodeur est autorisé à mémoriser ; quand il n'est pas renseigné, NBCA est défini par l'implémentation du module logiciel dans le décodeur selon l'invention

10 - LCA (Liste de cartes autorisées) : ce paramètre impose à un décodeur la liste des identifiants de cartes avec lesquelles il peut fonctionner.

15 - Perturbation : ce paramètre décrit la perturbation à appliquer par le décodeur dans l'accès aux données en cas de carte non appariée avec le décodeur.

20 Les paramètres fonctionnels ci-dessus sont organisés librement dans l'ensemble de paramètres FUNCTIONS 32. Une implémentation préférée est la combinaison de ces paramètres par structure T L V (Type Longueur Valeur).

FONCTIONNEMENT

25 Le fonctionnement de l'appariement selon l'invention va maintenant être décrit par référence aux figures 5 et 6.

 La figure 5 est un diagramme fonctionnel illustrant schématiquement les états de la fonction d'appariement du logiciel de contrôle d'accès 4 embarqué dans un décodeur 2.

30 La fonction d'appariement est dans l'état inactif 60 quand le logiciel de contrôle d'accès 4

vient d'être installé ou téléchargé (étape 61) ou quand il a reçu de la plateforme 1 un ordre de désactivation de l'appariement (étape 62) ou de réinitialisation de l'appariement (étape 64). Dans cet état le logiciel de
5 contrôle d'accès 4 accepte de fonctionner avec une carte 6 insérée dans le décodeur 2 sans vérifier son appariement avec cette carte.

Pour effectuer l'activation de l'appariement dans un décodeur 2, l'opérateur définit
10 via la plateforme 1 un mode d'appariement (= actif), optionnellement le nombre maximum NBCA de cartes 6 susceptibles d'être appariées avec le décodeur 2 et le type de perturbation applicable dans l'accès aux données en cas d'échec de l'appariement. En fonction de
15 ces informations la plateforme 1 génère et émet (flèche 68) un message EMM adressant le ou les décodeurs concernés et contenant les paramètres de configuration. La fonction d'appariement dans le décodeur passe à l'état actif 70.

20 L'opérateur peut désactiver l'appariement dans le décodeur 2, via la plateforme 1 qui génère et émet (flèche 72) un message EMM adressant le ou les décodeurs concernés et contenant un ordre de désactivation sans effacement du contexte d'appariement
25 62 ou un ordre de RAZ du contexte d'appariement 64. La fonction d'appariement dans le décodeur passe à l'état inactif 60.

Quel que soit l'état inactif ou actif de la fonction d'appariement, elle peut recevoir (étape 74)
30 une liste de cartes autorisées LCA par EMM émise par la plateforme 1.

La prise en compte d'une carte 6 par la fonction d'appariement dans un décodeur 2 est décrite dans l'organigramme de la figure 6.

5 A l'insertion (étape 80) d'une carte 6 dans le décodeur 2, le logiciel de contrôle d'accès 4 embarqué dans le décodeur teste (étape 82) si la fonction d'appariement est dans l'état actif 70.

10 Si la fonction d'appariement dans le décodeur est dans l'état inactif 60, le décodeur accepte de fonctionner avec la carte insérée (étape 92).

15 Si la fonction d'appariement dans le décodeur est dans l'état actif 70, le logiciel de contrôle d'accès lit l'identifiant de la carte et vérifie (étape 84) si cet identifiant de la carte insérée est déjà mémorisé dans le décodeur 2. Si l'identifiant de cette carte 6 est déjà mémorisé dans le décodeur 2, le logiciel de contrôle d'accès 4 accepte de fonctionner avec la carte insérée (étape 20 92). Dans ce cas, l'accès aux programmes diffusés est alors possible, sous réserve de conformité des autres conditions d'accès attachées à ces programmes.

25 Si l'identifiant de cette carte 6 n'est pas mémorisé dans le décodeur 2, le logiciel de contrôle d'accès vérifie (étape 86) si le nombre d'identifiants de cartes 6 déjà mémorisés est inférieur à la valeur maximum NBCA de cartes 6 autorisées par la configuration.

30 • Si ce nombre NBCA est atteint, le logiciel de contrôle d'accès 4 refuse de fonctionner avec la carte 6 insérée dans le lecteur du décodeur

2, et applique (étape 90) la perturbation dans l'accès aux données telle que définie par l'opérateur. Une telle perturbation peut consister à bloquer l'accès aux programmes diffusés. Elle peut être accompagnée de l'affichage sur l'écran du terminal auquel est associé le décodeur 2 d'un message invitant l'abonné à insérer une autre carte 6 dans le décodeur 2,

- 10 • Si ce nombre NBCA n'est pas atteint, l'identifiant de la carte 6 insérée dans le lecteur du décodeur 2 est ajouté à la liste des identifiants mémorisés (étape 88). Le logiciel de contrôle d'accès 4 accepte ensuite de
- 15 fonctionner avec la carte 6 insérée (étape 92).

Quand la carte 6 est extraite (étape 94) du décodeur 2, le logiciel de contrôle d'accès 4 passe en attente de l'insertion d'une carte 6 (étape 80).

La perturbation 90 dans l'accès aux données en cas de défaut d'appariement peut être de différente nature telle que par exemple :

- Arrêt audio et vidéo sur les chaînes cryptées (obtenu par non soumission des ECM à la carte pour calcul des CW) ;

25 - Arrêt audio et vidéo sur les chaînes en clair et analogiques (obtenu par message au middleware) ;

- Envoi d'un message au middleware du terminal (exemple : message Open TV).

30 Cette perturbation peut être utilisée également pour provoquer le blocage de décodeurs volés.

Dans le cas décrit dans la figure 2 où le logiciel de contrôle d'accès 4 est exécuté dans l'interface amovible 8 connectée à un décodeur 2, l'automate décrit dans la figure 4 et l'organigramme 5 décrit dans la figure 5 s'appliquent directement au logiciel de contrôle d'accès embarqué 4 dans cette interface amovible 8.

REVENDICATIONS

1. Procédé d'appariement d'un équipement récepteur de données numériques (2) avec une pluralité de modules externes de sécurité (6, 8) ayant chacun un
5 identifiant unique, procédé caractérisé en ce qu'il comporte les étapes suivantes :

- connecter un module externe de sécurité (6, 8) à l'équipement récepteur,
- mémoriser à la volée dans l'équipement
10 récepteur (2) l'identifiant unique du module de sécurité (6, 8) connecté.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre une phase de contrôle consistant à vérifier, à chaque connexion
15 ultérieure d'un module externe de sécurité (6, 8) à l'équipement récepteur (2), si l'identifiant dudit module est mémorisé dans cet équipement récepteur (2).

3. Procédé selon la revendication 2, caractérisé en ce qu'il comporte en outre une étape
20 consistant à transmettre à l'équipement récepteur (2) une signalisation comportant au moins un message de gestion de la mémorisation de l'identifiant du module externe de sécurité (6, 8) et/ou un message de gestion de la phase de contrôle.

4. Procédé selon la revendication 3, caractérisé en ce que ladite signalisation comporte au
25 moins une des consignes suivantes :

- autoriser la mémorisation,
- interdire la mémorisation,
- 30 - effacer les identifiants déjà mémorisés dans l'équipement récepteur (2),

- activer ou désactiver la phase de contrôle.

5 5. Procédé selon la revendication 3, caractérisé en ce que ladite signalisation comporte en outre le nombre maximal d'identifiants dont la mémorisation est autorisée.

10 6. Procédé selon la revendication 3, caractérisé en ce que ladite signalisation comporte une consigne de reconfiguration par laquelle on transmet à l'équipement récepteur (2) une liste mise à jour des identifiants des modules externes de sécurité (6, 8) appariés avec ledit équipement récepteur (2).

15 7. Procédé selon la revendication 6, caractérisé en ce que ladite liste est transmise directement à l'équipement récepteur (2).

8. Procédé selon la revendication 6, caractérisé en ce que ladite liste est transmise via un module externe de sécurité (6, 8) connecté audit équipement récepteur (2).

20 9. Procédé selon la revendication 2, dans lequel ladite phase de contrôle comporte une procédure consistant à perturber le traitement des données si l'identifiant du module externe de sécurité (6, 8) connecté n'est pas préalablement mémorisé l'équipement récepteur (2).

25 10. Procédé selon la revendication 1, caractérisé en ce que lesdites données sont distribuées en clair ou embrouillées par un mot de contrôle chiffré, et en ce que chaque module externe de sécurité
30 (6, 8) comporte des droits d'accès auxdites données et un algorithme de déchiffrement dudit mot de contrôle.

11. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation est transmise à un équipement récepteur (2) dans un message EMM spécifique à un module externe de sécurité (6, 8) associé à cet équipement récepteur (2).

12. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation est transmise à un équipement récepteur (2) dans un message EMM spécifique à cet équipement récepteur (2).

10 13. Procédé selon la revendication 6, caractérisé en ce que, pour un équipement récepteur (2) donné, ladite liste est transmise dans un message EMM spécifique à un module de sécurité (6, 8) associé à cet équipement récepteur (2).

15 14. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation est transmise à un groupe d'équipements récepteurs (2) dans un message EMM spécifique à un groupe de modules externes de sécurité (6, 8) associés auxdits
20 équipements récepteurs (2).

15 15. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation est transmise à un groupe d'équipements récepteurs (2) dans un message EMM spécifique audit groupe d'équipements
25 récepteurs (2).

30 16. Procédé selon la revendication 6, caractérisé en ce que, pour un groupe d'équipements récepteurs (2) donné, ladite liste est transmise dans un message EMM spécifique à un groupe de modules externes de sécurité (6, 8) associées auxdits équipements récepteurs (2).

17. Procédé selon l'une des revendications 4 ou 5, caractérisé en ce que ladite signalisation de contrôle est transmise dans un flux privé à un groupe d'équipements récepteurs (2).

5 18. Procédé selon la revendication 6, caractérisé en ce que, pour un groupe d'équipements récepteurs (2) donné, ladite liste est transmise dans un flux privé à chaque équipement récepteur (2).

10 19. Procédé selon l'une des revendications 17 ou 18, caractérisé en ce que ledit flux privé est traité par un logiciel dédié exécutable dans chaque équipement récepteur (2) en fonction de l'identifiant du module externe de sécurité (6, 8) qui lui est associé.

15 20. Procédé selon l'une des revendications 11 à 16, caractérisé en ce qu'il comporte en outre un mécanisme destiné empêcher l'utilisation d'un EMM transmis à un même module externe de sécurité (6, 8) dans deux équipements récepteurs (2) distincts.

20 21. Procédé selon l'une des revendications 11 à 13, caractérisé en ce que ledit EMM présente le format suivant :

```

25      EMM-U_section() {
          table_id = 0x88                8 bits
          section_syntax_indicator = 0   1 bit
          DVB_reserved                   1 bit
          ISO_reserved                   2 bits
          EMM-U_section_length           12 bits
          unique_adress_field            40 bits
30      for (i=0; i<N; i++) {
          EMM_data_byte                  8 bits
          }
      }

```

22. Procédé selon l'une des revendications 14 à 16, caractérisé en ce que ledit EMM est spécifique à tous les modules externes de sécurité (6, 8) ou à tous les équipements récepteurs (2) et présente le format suivant :

```

5      EMM-G_section() {
          table_id = 0x8A ou 0x8B           8 bits
          section_syntax_indicator = 0     1 bit
          DVB_reserved                      1 bit
10         ISO_reserved                    2 bits
          EMM-G_section_length             12 bits
          for (i=0; i<N; i++) {
              EMM_data_byte                8 bits
          }
15     }

```

23. Procédé selon l'une des revendications 14 à 16, caractérisé en ce que ledit EMM est spécifique à un sous-groupe de modules externes de sécurité (6, 8) ou d'équipements récepteurs (2) et présente le format suivant :

```

20      EMM-S_section() {
          table_id = 0x8E                   8 bits
          section_syntax_indicator = 0     1 bit
          DVB_reserved                     1 bit
25         ISO_reserved                    2 bits
          EMM-S_section_length             12 bits
          shared_address_field             24 bits
          reserved                         6 bits
          data_format                      1 bit
30         ADF_scrambling_flag             1 bit
          for (i=0; i<N; i++) {
              EMM_data_byte                8 bits
          }
      }

```

24. Procédé selon la revendication 1, caractérisé en ce que les identifiants de modules externe de sécurité (6, 8) sont groupés dans une liste chiffrée.

5 25. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce que l'équipement récepteur (2) comporte un décodeur et le module externe de sécurité (6, 8) comporte une carte de
10 contrôle d'accès (6) dans laquelle sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur, et en ce que l'appariement est effectué entre ledit décodeur et ladite carte (6).

15 26. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce que l'équipement récepteur (2) comporte un décodeur et le module externe de sécurité (6, 8) comporte une interface de sécurité amovible (8) munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec
20 le décodeur, et d'autre part, avec une pluralité de cartes de contrôle (6) d'accès conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur, et en ce que l'appariement est effectué entre ledit décodeur et ladite interface (8) de
25 sécurité amovible.

27. Procédé selon l'une quelconque des revendications 1 à 24, caractérisé en ce que l'équipement récepteur (2) comporte un décodeur muni d'une interface de sécurité amovible (8) ayant une
30 mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une

pluralité de cartes de contrôle (6) d'accès conditionnel et en ce que l'appariement est réalisé entre ladite interface de sécurité amovible (8) et lesdites cartes de contrôle d'accès (6).

5 28. Procédé selon la revendication 10, caractérisée en ce que les données sont des programmes audiovisuels.

29. Equipement récepteur (2) susceptible d'être apparié avec une pluralité de modules externes
10 de sécurité (6, 8) pour gérer l'accès à des données numériques distribuées par un opérateur, caractérisé en ce qu'il comporte des moyens pour mémoriser à la volée l'identifiant de chaque module externe de sécurité (6, 8) qui lui est connecté.

15 30. Equipement selon la revendication 29, caractérisé en ce qu'il comporte un décodeur et en ce que le module externe de sécurité (6, 8) est une carte de contrôle d'accès (6) comportant des informations relatives aux droits d'accès d'un abonné auxdites
20 données numériques, l'appariement étant effectué entre ledit décodeur et ladite carte (6).

31. Equipement selon la revendication 29, caractérisé en ce qu'il comporte un décodeur et en ce que le module externe de sécurité (6, 8) est une
25 interface de sécurité amovible (8) munie d'une mémoire non volatile et destinée à coopérer, d'une part, avec ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle d'accès conditionnel (6), pour gérer l'accès auxdites données numériques, l'appariement
30 étant effectué entre ledit décodeur et ladite interface de sécurité amovible (8).

32. Equipement selon la revendication 29, caractérisé en ce qu'il comporte un décodeur muni d'une interface de sécurité amovible (8) ayant une mémoire non volatile et destinée à coopérer, d'une part, avec
5 ledit décodeur, et d'autre part, avec une pluralité de cartes de contrôle (6) d'accès conditionnel et en ce que l'appariement est réalisé entre ladite interface de sécurité amovible (8) et lesdites cartes de contrôle d'accès (6).

10 33. Décodeur susceptible de coopérer avec une pluralité de modules externes de sécurité (6, 8) pour gérer l'accès à des programmes audiovisuels distribués par un opérateur, chaque module externe de sécurité (6, 8) ayant un identifiant unique et
15 comportant au moins un algorithme de traitement de données, décodeur caractérisé en ce qu'il comporte des moyens pour mémoriser à la volée l'identifiant de chaque module externe de sécurité (6, 8) qui lui est connecté.

20 34. Décodeur selon la revendication 33, caractérisé en ce que lesdits modules externes de sécurité (6, 8) sont des cartes de contrôle d'accès (6) dans lesquelles sont mémorisées des informations relatives aux droits d'accès d'un abonné à des données
25 numériques distribuées par un opérateur.

35. Décodeur selon la revendication 33, caractérisé en ce que lesdits modules externes de sécurité (6, 8) sont des interfaces de sécurité amovibles (8) comportant une mémoire non volatile et
30 destinées à coopérer, d'une part, avec le décodeur, et d'autre part, avec une pluralité de cartes de contrôle

d'accès (6) conditionnel pour gérer l'accès à des données numériques distribuées par un opérateur.

36. Interface de sécurité amovible (8) comportant une mémoire non volatile et destinée à coopérer, d'une part, avec un équipement récepteur (2), et d'autre part, avec une pluralité de cartes de contrôle d'accès (6) conditionnel, pour gérer l'accès à des données numériques distribuées par un opérateur, chaque carte (6) ayant un identifiant unique et comportant des informations relatives aux droits d'accès d'un abonné auxdites données numériques, interface caractérisée en ce qu'elle comporte des moyens pour enregistrer à la volée l'identifiant de chaque carte de contrôle d'accès (6) dans ladite mémoire non volatile.

37. Interface selon la revendication 36 caractérisée en ce qu'elle consiste en une carte PCMCIA comportant un logiciel de désembrouillage de données numériques.

38. Interface selon la revendication 36 caractérisée en ce qu'elle consiste en un module logiciel.

39. Programme d'ordinateur exécutable dans un équipement récepteur (2) susceptible de coopérer avec une pluralité de modules externes de sécurité (6, 8) ayant chacun un identifiant unique et dans lesquels sont stockées des informations relatives aux droits d'accès d'un abonné à des données numériques distribuées par un opérateur, caractérisé en ce qu'il comporte des instructions pour mémoriser à la volée

l'identifiant de chaque module externe de sécurité (6, 8) connecté audit équipement récepteur (2).

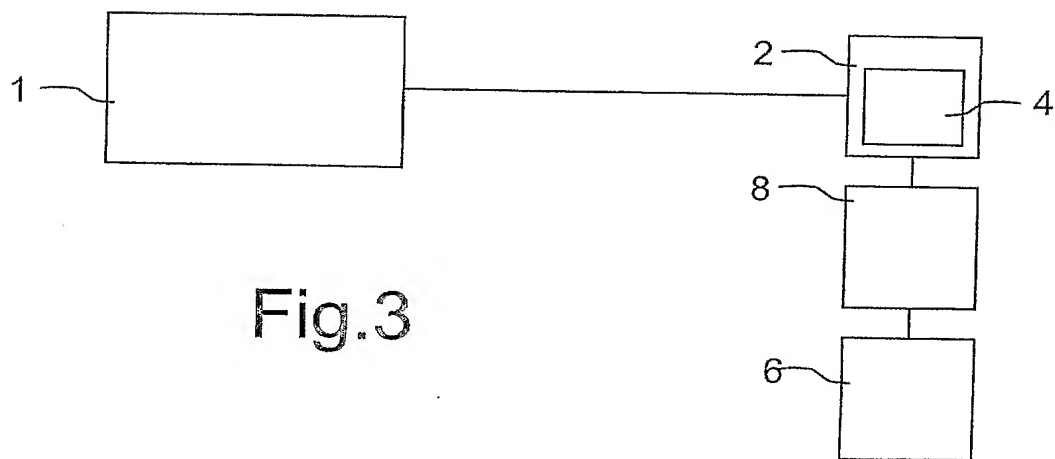
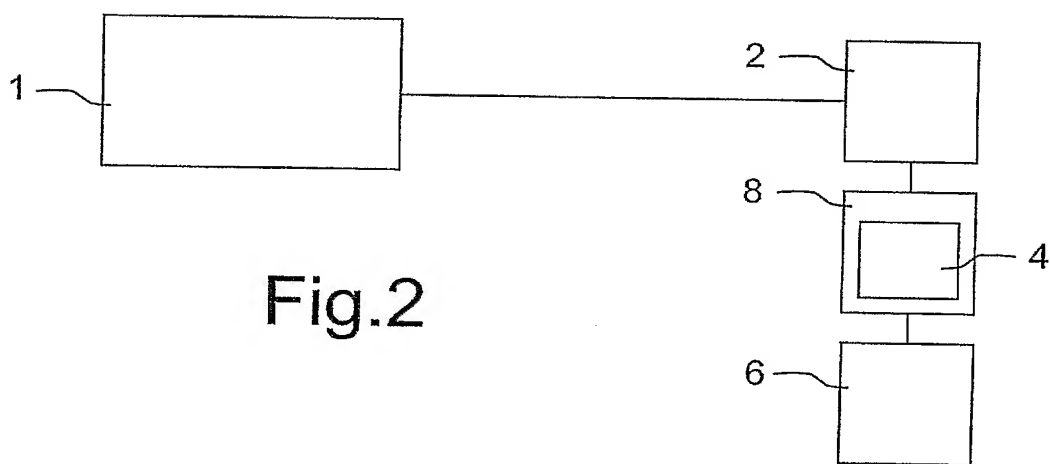
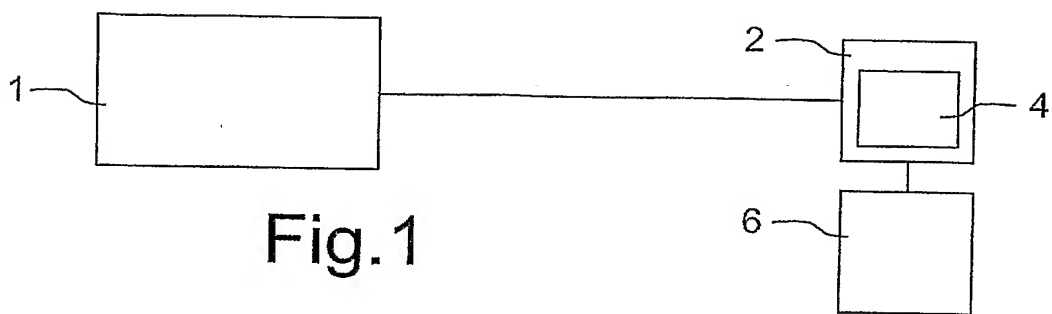
5 40. Programme d'ordinateur selon la revendication 39, caractérisé en ce qu'il comporte en outre des instructions destinées à générer localement des paramètres de contrôle de l'appariement de l'équipement récepteur (2) avec un module externe de sécurité (6, 8) en fonction d'une signalisation transmise audit équipement récepteur (2) par
10 l'opérateur.

41. Programme d'ordinateur selon la revendication 39, caractérisé en ce qu'il comporte en outre des instructions destinées à vérifier, à chaque utilisation ultérieure d'un module externe de sécurité
15 (6, 8) avec l'équipement récepteur (2), si l'identifiant dudit module externe de sécurité (6, 8) est mémorisé dans l'équipement récepteur (2).

42. Système comportant une pluralité d'équipements récepteurs (2) connectés à un réseau de
20 diffusion de données et/ou services, chaque équipement récepteur (2) étant susceptible d'être apparié avec une pluralité de modules externes de sécurité (6, 8), ledit système comportant également une plateforme de gestion commerciale (1) communiquant avec les équipements
25 récepteurs (2) et avec lesdits modules externes de sécurité (6, 8), caractérisé en ce qu'il comporte en outre :

- un premier module agencé dans ladite plate-forme de gestion commerciale (1) et destiné à
30 générer des requêtes d'appariement,

- et un deuxième module agencé dans lesdits équipements récepteurs (2) et destiné à traiter lesdites requêtes pour préparer une configuration de l'appariement et pour contrôler l'appariement.



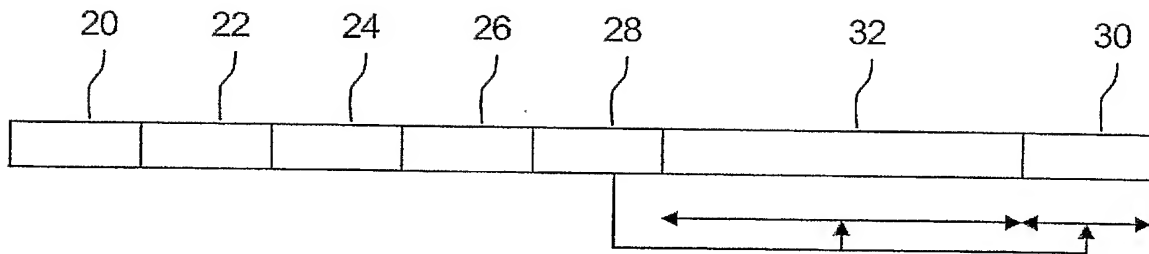


Fig.4

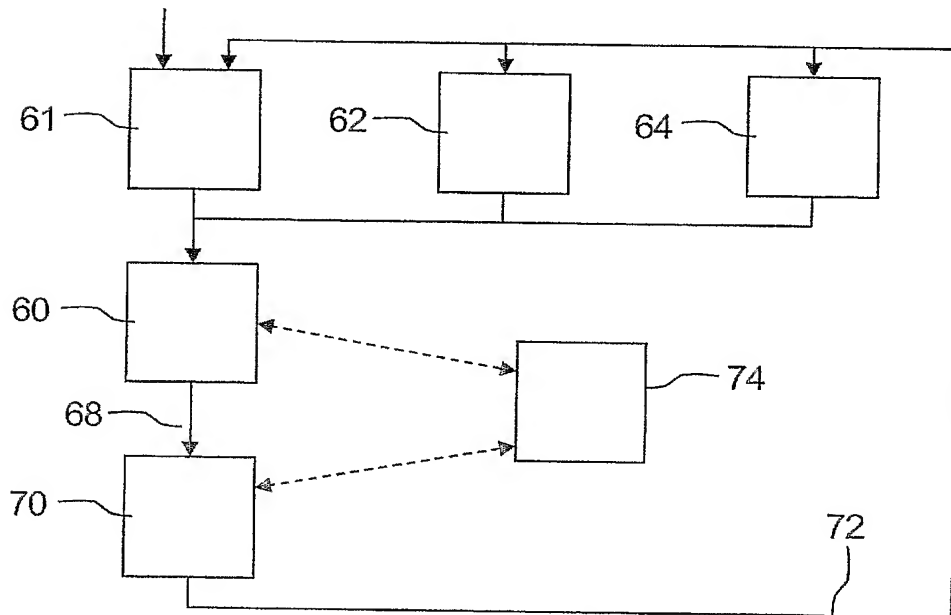


Fig.5

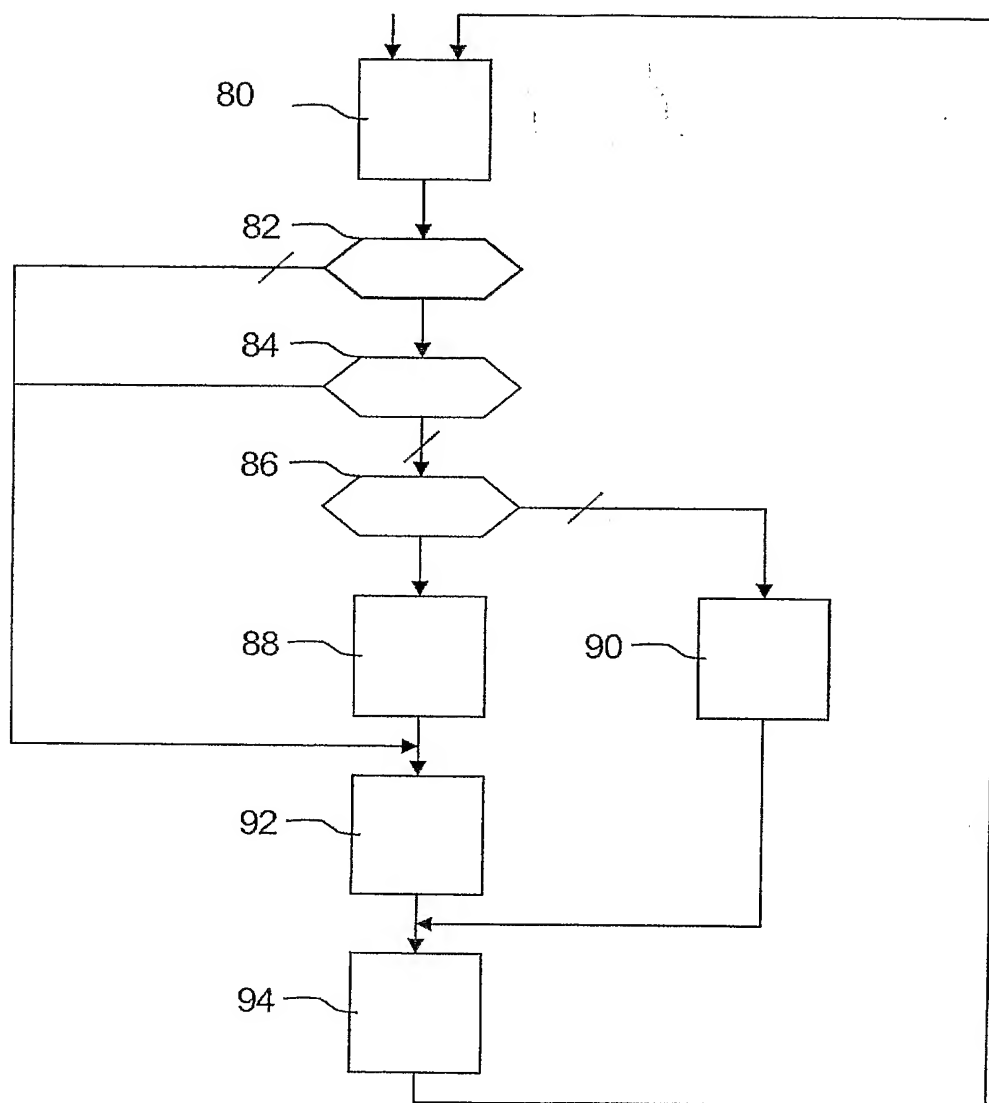


Fig.6



BREVET D'INVENTION CERTIFICAT D'UTILITE

Désignation de l'inventeur

Vos références pour ce dossier	SP 24282 HM 03-021
N°D'ENREGISTREMENT NATIONAL	04.50323 du 20.02.2004
TITRE DE L'INVENTION	
	PROCEDE D'APPARIEMENT D'UN TERMINAL RECEPTEUR AVEC UNE PLURALITE DE CARTES DE CONTROLE D'ACCES
LE(S) DEMANDEUR(S) OU LE(S) MANDATAIRE(S):	
DESIGNE(NT) EN TANT QU'INVENTEUR(S):	
Inventeur 1	
Nom	BEUN
Prénoms	Frédéric
Rue	30, avenue Guy de Maupassant
Code postal et ville	78400 CHATOU - FRANCE
Société d'appartenance	
Inventeur 2	
Nom	BOUDIER
Prénoms	Laurence
Rue	30, avenue Guy de Maupassant
Code postal et ville	78400 CHATOU - FRANCE
Société d'appartenance	
Inventeur 3	
Nom	ROQUE
Prénoms	Pierre
Rue	127, rue du Cherche Midi
Code postal et ville	75015 PARIS - FRANCE
Société d'appartenance	
Inventeur 4	
Nom	TRONEL
Prénoms	Bruno
Rue	9 rue de l'Oasis
Code postal et ville	92800 PUTEAUX
Société d'appartenance	

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

PARIS LE 08 AVRIL 2004

J.C. ILGART
97 0201

100 100 100

FR 05/050101

